Secure Element

STM32 Security Tool Box

STSAFE Secure Element

Ecosystem Partners

Demo
STM32-based IoT Node
Classes of Attacks

- **IoT Device**
  - Internet
  - Cloud Service
  - Software Attack
    - Misuse of network protocols
      - Exploit communication protocol errors
    - Flaws in software design / implementation

- **Board-Level Attack**
  - With the case opened / removed
    - Test / debug port access
    - Inter device bus and IO probing
    - Reset, clock attacks
    - Power analysis
    - Temperature / electrical attacks (glitch, overvoltage)

- **Silicon-Level Attack**
  - Device de-packaged
    - Circuit analysis and probing
  - Fault injection
    - Laser beam
Platform Security

The platform’s integrity is based on STM32 security tools
# STM32 Family Security Tools

## Security Features

<table>
<thead>
<tr>
<th>ST Family</th>
<th>Debug Access Port</th>
<th>RESET Register</th>
<th>FLASH WRPE</th>
<th>FLASH Mass ERASE</th>
<th>Tamper Pins</th>
<th>CRC Hardware</th>
<th>96-Bit Unique ID</th>
<th>Crypto Library</th>
<th>Support Memory Protection Unit(MPU)</th>
<th>FLASH RDP</th>
<th>TRNG</th>
<th>AES Hardware Accelerator</th>
<th>FLASH PCROP</th>
<th>HASH Hardware Accelerator</th>
<th>Firewall</th>
<th>SRAM RDP</th>
<th>FLASH ECC</th>
<th>Sys Clock (MHz)</th>
<th>ARM Cortex®</th>
</tr>
</thead>
<tbody>
<tr>
<td>STM32 F1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>72</td>
<td>M3</td>
</tr>
<tr>
<td>STM32 F3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>72</td>
<td>M4</td>
</tr>
<tr>
<td>STM32 F0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>48</td>
<td>M0</td>
</tr>
<tr>
<td>STM32 L1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>32</td>
<td>M3</td>
</tr>
<tr>
<td>STM32 F2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>120</td>
<td>M3</td>
</tr>
<tr>
<td>STM32 F4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>180</td>
<td>M4</td>
</tr>
<tr>
<td>STM32 F7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>216</td>
<td>M4</td>
</tr>
<tr>
<td>STM32 L0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>32</td>
<td>M0+</td>
</tr>
<tr>
<td>STM32 L4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>80</td>
<td>M4</td>
</tr>
</tbody>
</table>
Security Framework

- Use the STM32 Security Tools to develop a layered security solution
Secure Solutions

STSAFE enabling end-to-end security

- **STSAFE-A Optimized authentication solution**
  - Authentication
  - Secure communications, Secure data storage
  - Secure key provision service
  - EAL5+ Common criteria certified chip

- **STSAFE-J Flexible Java-based solution**
  - Trusted network access with Authentication
  - Secure Data storage, Secure communication
  - Personalization services
  - Common criteria and BSI certification

- **STSAFE-TPM Standardized solution**
  - Platform integrity, Authentication
  - Secure Boot, Secure Firmware upgrade
  - Secure data storage and Secure communication
  - Solution CC EAL4+ and TCG 1.2 / 2.0 certified
Classes of Attacks

- **IoT Device**
  - Internet

- **Cloud Service**
- **Remote Software Attack**
  - Misuse of network protocols
  - Exploit communication protocol errors
  - Flaws in software design / implementation

- **Board Level Attack**
  - With the case opened / removed
  - Test / debug port access
  - Inter device bus and IO probing
  - Reset, clock attacks
  - Power analysis
  - Temperature / electrical attacks (glitch, overvoltage)

- **Silicon Level Attack**
  - Device de-packaged
  - Circuit analysis and probing
  - Fault injection
  - Laser beam
Enhanced Platform Security

STSAFE adding enhanced tamper-resistance
Adding a Secure Element

STSAFE Supporting Secure Boot, Firmware Updates and Communication

- A Secure Element is designed to thwart silicon invasive attacks
- Independently assessed, achieving very high standards like EAL5+ Common Criteria Certified chip
- Protects keys and performs cryptographic functions (ECDH, ECDSA, AES)
  - For Secure Communications, Boot and Firmware Updates
- Provides up to 6K bytes Secure Data Store
- Secure keys and certificates are provisioned during the manufacturing process
- STM32 SDK available
STSAFE-A100 improves TLS performance

STSAFE integrated with WolfSSL

Benchmark - Time

- ECC 256 key gen
- ECDHE 256 agree
- ECDSA 256 sign
- ECDSA 256 verify

Faster is better!
Security Ecosystem Partners

Ecosystem of unique technologies, services and solutions

Together, helping to realize your secure product solution

- Firmware Libraries
- Consultancy and Engineering Services
- Training and Tools
- Security Assessment
- Modules and Cloud Solutions
- Device Provisioning/Personalization
Security Ecosystem Partners
Boot Loader uses STSAFE for crypto off-load, PKI attestation, and secure data storage.

Windows based Software Update Management Station generates STSAFE key material.

SE Profile Station personalizes the STSAFE, using custom STSAFE test fixture.

Cypherbridge’s custom STSAFE
uLoadXL + SE Solution

- Secure Boot Loader managing multiple images
- Managed safe / secure software update
- Anti-cloning, system integrity and safety
- Application image encryption, hash integrity and authentication, code sign and verify
- System Availability provides application integrity, auto-rollback, failsafe boot
Cloud Connectivity - Out Of The Box!

Pre-integrated ST Firmware Packages

Single board using ST Hardware Building Blocks

AWS IoT

Microsoft Azure IoT

IBM Watson IoT

STM32L475 Discovery Kit IoT Node
STM32L475 Discovery kit IoT node

Main features
- Expandable to allow ST sensor technology (Motion MEMS) data to be published to the cloud for data analysis
- AWS IoT Core or AWS Greengrass connection

- Ready to run firmware example using Wi-Fi connectivity to support quick evaluation and development of AWS IoT cloud applications
- Amazon FreeRTOS and AWS IoT Device SDK Firmware packages (X-CUBE-AWS)
Microsoft Azure IoT Demo

STM32L475 Discovery kit IoT node

- Ready to run firmware example using Wi-Fi connectivity to support quick evaluation and development of Microsoft Azure IoT
- Azure IoT device SDK packages available (X-CUBE-AWS, FP-CLD-AZURE1 also compatible with Microsoft IoT Central)

Main features
- Expandable to allow ST sensor technology (Motion MEMS) data to be published to the cloud for data analysis
- Ready-to-use binaries to connect the IoT node to STM32ODE IoT web dashboard running on Microsoft Azure, for sensor data visualization, LED control and device management (FW Over-The-Air Update)
Main features

- Expandable to allow ST sensor technology (Motion MEMS) data to be published to the cloud for data analysis
- Bidirectional communication examples between the board, acting as a device, and the IBM Watson IoT™ platform

- Ready-to-run firmware example using Wi-Fi connectivity to support quick evaluation and development of applications on the IBM Watson IoT platform
- IBM Watson IoT Embedded C SDK packages available (X-CUBE-WATSON, FP-CLD-WATSON1)
STM32L4 Discovery kit IoT node, low-power wireless, BLE, NFC, SubGHz, Wi-Fi

SW Libraries for STM32L4 MCU & Sensors

Low-power, long-range communication

Direct Wi-Fi connection to cloud servers

Environmental awareness: humidity, pressure, temp

Detection hub: motion, proximity, audio
STM32 High Performance

Audio Front End

STM32F7 with 2-microphone speech recognition based on Sensory’s trigger-word recognition and DSP-Concepts audio front end

Audio Front end with Acoustic Echo Cancellation, Beamforming, Source Localization and Noise Reduction

The STM32 audio front end connected via gateway to AVS